Technical Information

TI 04L51B01-04EN

SMARTDAC+
Advanced Security Functions
White Paper for FDA 21 CFR Part 11

Part 11

For FDA 21 CFR PART 11

The contents of this Technical Information are subject to change without notice.

YOKOGAWA

Yokogawa Electric Corporation
2-9-32, Nakacho, Musashino-shi, Tokyo, 180-8750 Japan

TI 04L51B01-04EN
©Copyright May. 2014
1st Edition May 15, 2014

Contents

Introduction 3

1. Overview of 21 CFR Part 11 4
2. Industry Support to Comply with the Regulation 5
3. Overview of 21 CFR Part 11 Requirements and their Incorporation into the Features of the SMARTDAC+ GX10/GX20, GP10/GP20 Advanced Security Functions (/AS): 6
4. Electronic Signature Security and Manifestation Requirements ... 11
5. Other Procedural Controls 15

Revision Information i

All Rights Reserved. Copyright © 2014, Yokogawa Electric Corporation

Introduction

This document describes the Advanced Security Functions.

■ Notice

- The contents of this manual are subject to change without notice as a result of continuing improvements to the instrument's performance and functions.
- Every effort has been made to ensure accuracy in the preparation of this manual. Should any errors or omissions come to your attention, however, please inform Yokogawa Electric's sales office or sales representative.
- Under no circumstances may the contents of this manual, in part or in whole, be transcribed or copied without our permission.

■ Trademarks

- Our product names or brand names mentioned in this manual are the trademarks or registered trademarks of Yokogawa Electric Corporation (hereinafter referred to as YOKOGAWA).
- Ethernet is a registered trademark of XEROX Corporation in the United States.
- We do not use the TM or ® mark to indicate these trademarks or registered trademarks in this user's manual.
- All other product names mentioned in this user's manual are trademarks or registered trademarks of their respective companies.

1. Overview of 21 CFR Part 11

21 CFR§ 11, the FDA's final rule on Electronic Records and Electronic Signatures, (Part 11) was developed in part in response to industry demand and in part as a result of regulations requiring government agencies to implement policies to reduce the amount of paperwork both reviewed and stored in archives. Promulgated in August, 1997, Part 11 provides the criteria under which the FDA will consider electronic records and signatures to be equivalent to conventional paper records and handwritten signatures.

Comparison of Paper-Based Controls with Requirements for Electronic Records under 21 CFR § 11:

Just as there are requirements for paper-based systems to assure that records are maintained in a secure form, protected from unauthorized changes and physical deterioration, Part 11 provides controls to assure that electronic records can be maintained in the same way. Just as in a paper-based system changes may not obliterate the original entry, changes made to an electronic record may not obscure the original. In a paper-based system, all changes must be attributable to an individual, and in an electronic record system all changes made must be recorded in an audit trail that traces those changes back to an authorized user of the system. Physical security controls must be in place to prevent unauthorized access to both paper-based and electronic records, and additional logical security procedures must be implemented to further protect electronic records from unauthorized access.

Requirements for record archives are the same in both paper-based and electronic record systems. Both must be maintained in such a manner that they can be retrieved for the duration of the required storage period.

Electronic signatures applied to electronic records and conventional handwritten signatures applied to electronic records are recognized by the FDA as having the same legal authority as conventional handwritten signatures applied to paper records. Thus, appropriate controls are needed over signatures that are applied to electronic records to assure that they cannot be forged or copied to a different record. Additionally, it is necessary to provide a means of verifying, during any routine review or inspection, that an electronic record has been signed in the same way that a signed paper record provides immediate proof that it has been signed by virtue of the prominently displayed signature.

Part 11 also requires organizations and individuals utilizing electronic records and/or electronic signatures to implement procedural controls to assure that affected personnel are appropriately trained and that all policies surrounding these records are properly documented.

Scope and Enforcement of 21 CFR § 11

While Part 11 is mandatory and not merely guidance from the FDA, it applies only to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under records requirements set forth in FDA regulations. The scope of the regulation covers both electronic records that will be submitted to the FDA and electronic records that are being kept to meet an FDA regulatory requirement even if they will not be directly submitted to the FDA.

Records that are maintained by a company, but not required to comply with any FDA regulation do not need to comply with Part 11.

2. Industry Support to Comply with the Regulation

Various support industries, such as those manufacturing automated laboratory instruments, are assisting regulated industries in achieving compliance by developing new and upgraded systems that include the logical controls needed to assure security and traceability of electronic records throughout the record's life-cycle. Yokogawa is one such company. Yokogawa has remained committed to providing the highest quality solutions and leading edge technologies in the fields of industrial automation, and test and measurement.

Yokogawa has recently undertaken a major revision and upgrade of its DAQSTATION DXAdvanced paperless recorders to provide features designed to meet the requirements of Part 11 for enhanced security and traceability of electronic records. The SMARTDAC+ with Advanced Security Functions (GX/AS) paperless recorders can be used in conjunction with an organization's own internal procedures to achieve full compliance with Part 11. Throughout this document, requirements that cannot be met solely by the automated system but also require internal procedural controls are inserted into sections titled "Administrative Alert/Procedural Control." At the end of this document, the text of Part 11 is incorporated into a summary table that can be used as a quick reference to determine compliance to specific sections of the regulation.

The GX/AS paperless recorders are designed to function independently to collect data from a variety of applications. They will integrate effectively into any environment in which conventional chart recorders are currently used. These versatile recorders can collect and integrate data from up to 500 individual input channels that can be individually, with an option of an additional 100 calculation channels and additional 500 communication channels. Data can be transferred to a secure directory on a company's network for further review via the SMARTDAC+ standard software, and also for archival and backups. Additionally, it is now possible for an appropriately authorized administrator to remotely configure the GX/AS using the SMARTDAC+ standard software's communicator module. Real-time data can be viewed remotely through a web interface, thus allowing closer monitoring and control of processes without the need to travel to a remote production floor .

3. Overview of 21 CFR Part 11 Requirements and their Incorporation into the Features of the SMARTDAC+ GX10/GX20, GP10/GP20 Advanced Security Functions (/AS):

Logical Security

Part 11 requires that access to systems that are used to create, modify, maintain, or retrieve electronic records to meet FDA requirements must be limited to authorized individuals. Additionally, authority checks are required to assure that authorized individuals accessing the systems are able to perform only tasks for which they have the appropriate level of access and for which they have been properly trained. (21 CFR 11.10(d), (g), (i))

The GX/AS paperless recorder can be configured to utilize a three-way combination of user name, user identification codes (user IDs), and password or a two-way combination of user name, and password to limit system access only to authorized users. Each user name must be unique, as must each combination of user ID and password. Permissions can be further defined to provide a variety of access levels ranging from view-only access to full administrative and remote communication and configuration rights.

Up to 100 users can be registered and divided as needed into system administrators or standard users. Individual users cannot modify their own access levels.

This security is maintained throughout the lifecycle of the electronic records in that the user permission and security data are directly linked to the associated acquired data files even when transferred via FTP, External memory, or other means to a more permanent storage location.

> Administrative Alert/Procedural Control: Each user must be properly trained to perform their assigned tasks. That training should be according to approved and available written policies and SOPs and must be documented. Training must encompass both the routine functions of the instrument and additional requirements imposed by the electronic nature of the data, including security. (21 CFR 11.10 (i))

Additional security is required when user name/user IDs and password combinations are used to apply electronic signatures to assure that these cannot be copied or used by anyone other than their genuine owners. To assure continued security of user name/user ID/ password combinations, identification codes and passwords must be periodically checked, recalled, or revised. (21 CFR 11.200(a)(2); 11.300(a), (b))

The GX/AS can be configured to use a combination of user name, user ID, and password to apply an electronic signature. While the user names and IDs can be viewed by administrators,

passwords are stored encrypted and cannot be viewed by anyone, including administrators. When a user account is initially configured by an administrator, the password is set to a

default pre-expired password for that user level. Upon initial login, and before gaining access to any functions on the GX/AS, the user is immediately prompted to change the password. The GX/AS requires entry of a minimum of 6 and a maximum of 20 alphanumeric characters or symbols. Empty spaces or null values are not allowed, and the password is case-sensitive. If required by company polices, the administrator can configure a user's password to periodically expire at 1-month, 3-months, or 6-month intervals.

Limiting system access to only authorized users and controlling individual levels of access provides effective security during periods of routine use of the instrument. Part 11 requires additionally that records be protected so that they can be retrieved readily and accurately throughout any required retention period. This requirement applies not only to records at their time of creation but also to archived electronic records for the duration of their storage period. (21 CFR 11.10(c))

An FTP client mode function allows records created by the GX/AS to be automatically sent to a secure FTP server directory. The GX/AS itself has the capability of automatically sending a preconfigured username and password combination, if required, for file upload access to the FTP directory. Data files are sent and received securely with SSL encryption via FTPS (File Transfer Protocol over SSL/TLS). Access levels at the FTP server, directory can be further controlled through good local network security policies. Neither the GX/AS nor the SMARTDAC+ standard software allow a user to overwrite records. Data files are stored sequentially to the GX/AS archive media (SD card) and then to the FTP server, when this function is used, so the data record is always archived even if a network connection to the server is lost. If the connection fails, data will be automatically transferred via FTP as soon as the connection is restored. These records can then be maintained under a company's general electronic records archive policies.

> Administrative Alert/Procedural Control: The GX/AS includes a FIFO (first-in-first-out) local data storage option that will automatically overwrite old data files on the local storage medium after the medium become full. If the local storage medium will be used for primary data storage, it is recommended that this feature be set to "Off" to assure proper long-term maintenance of critical electronic records.

Record Traceability and Audit Trails

As in paper-based systems, where changes made to records may not obliterate the original entry, changes made to electronic records also may not obscure previously recorded information. A secure, computer generated audit trail that automatically records the date and time of all operator entries and actions that create, modify, or delete electronic records serves to meet this requirement under Part 11. The FDA further clarified this requirement in the preamble to the regulation (FR vol. 62, No. 54, 3/20/97) where it described the intent of the audit trail as providing "a record of essentially who did what, wrote what, and when." The audit trail requirement under the regulation is designed to cover only those actions initiated by a person, not nonhuman background recordings made by an instrument or software application independent of operator input. Additionally, the audit trail needs to record all actions that change an electronic record in any way, but does not need to record user actions, such as switching among screen displays, that would have no effect on the content of electronic records. (21 CFR 11.10(e))

It is important not only to track changes made to acquired data such as temperature readings but also to track operator actions such as activating a manufacturing sequence or turning off an alarm. Because the FDA is interested in being able to reproduce and verify

the process under which data were acquired, any modification that would change the final result should also be tracked via an audit trail. This might include changes to calculations, calibration methods, or alarm settings. Because changes to user security settings could have a significant effect on the validity of data, these should also be traceable to the individual making the change and the date and time of the change. Such data can be loosely grouped under the term metadata.
Regardless of the mode of access or modification, the GX/AS maintains records of all alarms, alarm acknowledgements, error messages (including unauthorized attempts at access), changes to configuration and calculation settings, and current user authorization levels in binary files.
These files can be viewed through the SMARTDAC+ standard software but cannot be changed by users or administrators. Acquired data, such as temperature values, are also stored in a proprietary binary format and cannot be changed once they have been stored. Should a user attempt to change any data by directly accessing the binary data, the file will become useless to the user. An error message will appear the next time anyone attempts to access the data notifying the user that the data has been changed and the file cannot be viewed.

> Administrative Alert/Procedural Control: Procedures for backups and archives must be developed and implemented to assure that accurate copies of all data are securely maintained and can be retrieved for the entire required storage period. (21 CFR 11.10(b), (c))

The audit trail must be capable of being copied and available for review for the required storage period of the associated electronic record. (21 CFR 11.10(e))
Each log created by the GX/AS is linked to the next data file created after the change. The logs are copied automatically whenever the original data file is copied, and they are transferred to the FTP server for long-term storage along with the associated data file.

Validation

Systems used to create, modify, and maintain electronic records must be validated to ensure accuracy, reliability, consistent intended performance and the ability to discern invalid or altered records. (21 CFR 11.10(a))
While a significant amount of verification testing can be performed by the factory, to fully comply with agency expectations, validation of systems must be performed in their actual working environment. Therefore, no vendor can truly make a claim that any system has been fully validated for use in an FDA regulated environment. However, because each user will merely be choosing from a set list of functionality available with the GX/AS, it is possible to prepare both Installation/Configuration/Function verification protocols that can be completed by each user to meet their own specific requirements for functionality. Yokogawa is providing an Installation/Configuration/Function verification template at additional cost that can be used in conjunction with an end user's own operational policies and procedures to meet the requirements for validation of this system.

Record Maintenance

Part 11 requires that electronic records be protected to enable accurate and ready retrieval throughout their retention period. Additionally, it must be possible to make both electronic and human readable copies that are suitable for inspection, review, and copying by the

FDA. The copies must be accurate and complete so that it will be possible to create a virtual reproduction of the processes contributing to the original creation of the records. (21CFR 11.10(b))

Key to this requirement is the concept of metadata, or data about data. Metadata are those data in addition to the acquired results or measurements that determine the environment in which the acquired data are collected. In the environment of the GX/AS this includes, but is not limited to, information such as the actual identification make and model of the GX/AS used to collect the data, input channel settings, calibration settings, alarm settings, calculations programmed into the math channels, communication channel settings, user access levels, units of measurement, thermocouple types (collectively referred to as system settings), and dates and times of “start” and “stop” commands.

Metadata are stored completely in dedicated configuration files, and then copied into the next data file at the start of a run. This is the electronic audit trail data for the GX/AS. Because this information is automatically saved with the batch data files, maintenance of the metadata occurs naturally if the batch records are maintained.

Final secure maintenance of all GX/AS data can be further enhanced by using the FTP client mode feature. The GX/AS can transfer data files automatically to a secure network server. Primary and secondary servers can be specified. Files automatically transfer to the secondary server only if connection to the primary sever fails. When FTP client mode is used, the data file (including all audit trail data) is saved to both the archive media (SD card) and the server at the same time. Either location can be selected to serve as a master user copy, backup, or final archive. Various possible usage options are as follows:

Option 1: On memory stop action (end of data file/batch record) the instrument is configured to store the data to the archive media and to send a backup copy via FTP to a network server. Electronic signatures can be applied by SMARTDAC+ standard software to the file stored on the portable archive media. The same access security measures apply for both the GX/AS and SMARTDAC+ standard software under all conditions. With each modification of the locally stored media, an updated backup file is sent to the server via FTP. These backup files can be maintained and archived in accordance with a company’s established network backup procedures.

Administrative Alert/Procedural Control: The signature type can be set on individual batches for long-duration data acquisition, and if a batch's data is divided and stored into multiple files, those files cannot be signed without SMARTDAC+ standard software. This is described further under Electronic Signature Implementation in this document.

Option 2: The GX/AS is used in a completely stand-alone mode without using the FTP transfer feature. All data are stored to the internal memory and portable archive media. Data that is stored to the internal memory may serve as the master data and data that is stored to the archive media may serve as the master copy and ultimately the final archive. Records can be reviewed and signed later using the GX/AS or the SMARTDAC+ standard software by retrieving the appropriate file. Under this scenario, only a single working copy of each data file is available, and all modifications are applied to the same file, Backups can be performed through the company’s routine backup policies.

Administrative Alert/Procedural Control: Procedures, such as those governing creation of backups and archives, must be developed to assure that all electronic records are adequately protected throughout the required record retention period. (21 CFR 11.10(c))

Records maintained by the GX/AS and the SMARTDAC+ standard software are stored in a media format that can be easily copied for backups and archiving. Records can be securely stored in a network directory or other area with controlled access and then archived through a company's routine procedures to be readily available for inspection and copying for regulatory officials. Data created and stored by the GX/AS can be viewed only through the Yokogawa software, either locally at the GX/AS or remotely through the SMARTDAC+ standard software.

Administrative Alert/Procedural Control: Company change control, backup, archive, and disaster recovery policies should be sure to encompass both the GX/AS data files and the SMARTDAC+ standard software, if used.

Additional Controls for Open Systems

Part 11 acknowledges two basic categories of electronic record keeping systems, open and closed. A closed system is defined as an environment in which system access is controlled by the same persons responsible for the content of the electronic records maintained on that system. An open system is one in which system access is controlled by persons other than those responsible for the content of the records maintained on that system. Examples of closed systems include a stand-alone PC or a company's local network. An example of an open system is a system that may be accessed through an outside internet service provider. Because of the increased risk to data integrity and confidentiality when sent through an open system, Part 11 requires additional controls over that data that may include document encryption, or digital signatures.

The GX/AS functions as a stand-alone instrument and does not allow a user to access locally stored data remotely, nor can data be acquired anywhere other than at the local GX/AS station. The GX/AS status can be viewed remotely through Microsoft Internet Explorer but electronic data cannot be changed through this route. Remote configuration features available through the SMARTDAC+ standard software function only within the parameters of a company's local network.Thus, the GX/AS functions as a closed system with system access controlled by the same people responsible for the content of the associated electronic records, and additional security requirements for open systems as defined in Part 11 are not applicable. The SMARTDAC+ standard software can be used to access data that has been transferred to a network directory via FTP for reviewing and signing provided a user has been provided with sufficient access rights. The SMARTDAC+ standard software must be individually installed onto each PC on which it is used. If access to the company's network is controlled by the company, there are no additional concerns related to open systems associated with the GX/AS. (21 CFR 11.30)

4. Electronic Signature Security and Manifestation Requirements

Criteria have been set forth in Part 11 which, when met, will assure that electronic signatures applied to electronic records possess all characteristics necessary to be considered the legal equivalent of conventional handwritten signatures applied to paper records. Measures must be taken to assure that electronic signatures cannot be copied or forged through conventional means of electronic data manipulation.
Additionally, logical security features must be established to assure that electronic signatures cannot be applied by anyone other than their actual owners and can be traced unambiguously to a single individual. (21 CFR 11.70; 11.200(a)(2), (3); 11.300(a))

> Administrative Alert/Procedural Control: Before an organization may begin using electronic signatures, they must submit a signed statement to the FDA certifying that the electronic signatures in their system are intended to be the legally binding equivalent of traditional handwritten signatures. This certification must be submitted in paper form and may be submitted globally to cover all electronic signatures for the entire organization. Additional certification of individual electronic signatures must be submitted upon agency request. (21 CFR 11.100(c))

Required controls for electronic signatures vary depending upon the type of signature being applied. Signatures that are based solely on a series of keystrokes, such as a combination of user ID and password, require controls such as periodic password expiration to assure that they continue to be available only to the authorized user. Electronic signatures that involve a combination of keystrokes and use of a device or token require loss management controls and periodic performance checks to assure that they have not been tampered with. Additionally, these cannot be based solely upon a single element such as a swipe of a token or card, but must be combined with additional controls such as password entry or other feature to assure that, if stolen, they cannot be used by an unauthorized person. Electronic signatures based on biometrics, such as fingerprints or voice scans, are clearly the most secure form. However, these must be carefully designed to assure that they cannot be used by anyone other than their genuine owner. When fully compliant and secure, this type of electronic signature does not require a secondary confirmation such as a password. (21 CFR 11.300(b), (c); 11.200(b))

Electronic Signature Implementation in the GX/AS

The GX/AS recorders allow the application of electronic signatures that utilize a combination of the user's name, user ID, and password. Up to three (3) electronic signatures can be affixed to a data file, and each user is assigned an individual signature slot (Signature 1, Signature 2, Signature 3, or no signature authority) at the time of configuration. Users may only sign a record if their allotted slot has not already been filled. An administrator may sign in any signature position that has not been previously filled by another's signature.
On the GX/AS, you can choose whether to sign data by batch or by file. If the signature type is set to Batch, the data from start to finish must be contained in a single file.
In this mode, signatures may be applied directly at the GX/AS station, or with the SMARTDAC+ standard software during later record review on a computer. However, it is

possible for a batch record to consist of multiple files saved in sequence over a long time period. In this case, signatures may only be applied with the SMARTDAC+ standard software during later record review. The SMARTDAC+ standard software automatically links multiple files together within a batch and applies signature information to each file.
In Continuous mode, each data file is its own discrete entity. Signatures can be applied either at the GX/AS station or with the SMARTDAC+ standard software. Electronic signatures affixed to data collected in Continuous mode apply only to a single data file, not to an entire batch. And signatures can be applied to combined data file at the SMARTDAC+ standard software.

General Requirements for all Electronic Signatures

Each electronic signature must be uniquely traceable to a single individual and may not be re-used or reassigned to anyone else. (21 CFR 11.200(a)(2), (b))
On the GX/AS you can register up to 100 users and divide them as needed into system administrators or standard users.
It is not possible to duplicate user name and /or User ID and password combinations, thus each electronic signature will be uniquely traceable to a single individual.

> Administrative Alert/Procedural Control: Written policies must be established holding individuals using electronic signatures accountable and responsible for actions initiated under their electronic signatures. Internal training should emphasize the possible consequences of using another person's identification information and of sharing identification and password combinations with others. Additionally, a company is required to verify an individual's identity before authorizing them to use electronic signatures. This procedure can be easily incorporated into most human resources policies. (21 CFR 11.10(j); 11.100(b))

Electronic signatures that are not based on biometrics must use at least two distinct components. Examples are electronic signatures that utilize a combination of a User ID and password, or electronic signatures comprised of a swipe card plus password combination. One of those components must be executable only by the authorized user. When a user applies a series of electronic signatures during a single session of continuous controlled access, the initial signing must employ all of the electronic signature components. Subsequent signings during that same period of controlled access must employ the component that is executable only by the individual. If one or more signings are not performed during a single session of continuous controlled access, each component of the electronic signature must be applied each time. (21 CFR 11.200(a))
At its highest security level, the GX/AS utilizes a three-way combination of User Name, User ID, and password to allow routine user access. The electronic signature process automatically applies the user's name to the record after they have correctly entered their User ID and password. The password component is stored encrypted and is not available for viewing by anyone. When electronic signatures are used, each signature requires the user to reenter both the User ID and the password, thus there are no issues related to continuous versus non-continuous controlled access when operating the GX/AS. Signature application through the SMARTDAC+ standard software includes the same components and controls.
Electronic signatures must be administered and executed to assure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals. (21 CFR 11.200(a)(3))

The password component of the user's identification is stored in encrypted format and is not viewable to an administrator or other user.

In addition to entering characters on the GX/AS by using the touch screen, an optional USB keyboard is also available. As with all systems using passwords, users should be careful not to enter their private security codes when other personnel are watching.

Signature Manifestations

The printed name of the signer, the date and time of signing, and the meaning of the signing must be included as part of any human readable form of the electronic record. This includes both paper and electronic displays. The electronic signatures must be linked to their respective electronic records so that they cannot be removed, copied or transferred in any other way using ordinary means of record manipulation. (21 CFR 11.50, 70)

Before affixing an electronic signature to a data set, an authorized user is required to log onto the GX/AS or SMARTDAC+ standard software. The user name as originally entered is automatically applied to the electronic signature. The date and time of signing are automatically saved along with the signature. Calendar functions in the GX/AS can only be changed by an authorized administrator or authorized user, not by a routine user. When a user electronically signs a GX/AS data file, they are prompted to choose either "Pass" or "Fail" as a meaning of that signature and have the option of entering additional comments. Electronic signatures applied to records created by the GX/AS cannot be removed after they have been applied. GX/AS data files are stored in a proprietary binary format so that they cannot be modified by ordinary means once they have been created. This applies equally to the electronic signatures. The actual signatures and all associated data can be viewed either at the GX/AS or through the SMARTDAC+ standard software.

Administrative Alert/Procedural Control: A fully compliant electronic signature in the GX/AS environment requires that the full user's name is entered into the User Name field when the user is initially configured for access to the recorder. There is no minimum number of characters required in the User Name field, therefore this requirement should be specified in a company procedure to be sure that it is followed consistently.

Specific Controls for Identification Codes and Passwords

When used to apply electronic signatures, identification codes (user name and user ID) and passwords must be periodically checked, recalled, or revised to ensure continued confidentiality. Additionally, transaction safeguards are required to assure that any unauthorized attempts at use will be detected, reported, and prevented. It is insufficient to merely detect and report attempts at unauthorized use. The impostor must also be prevented from gaining access to the records for signing. (21 CFR 11.300(b), (d))

User passwords can be configured to expire at 1, 3, or 6-month intervals in the GX/AS. A user is not permitted to reenter the same password for more than one time-cycle. No user can electronically sign a record without first logging onto the GX/AS with an authorized user name/password combination. At login, a user is permitted only three (3) or five (5) attempts to enter a correct User ID/password combination. After the third or fifith incorrect attempt, that user's access permissions are deactivated and notification, depending on the system's

configuration, is sent. Following appropriate investigation, an administrator can acknowledge the warning message, re-set the user's access permissions, and allow the actual owner of the signature to use the instrument and electronically sign records.

> Administrative Alert/Procedural Control: Routine password expirations should be specified in written procedures and then incorporated into the user configuration of the GX/AS.

Further security is provided at the actual signature application level. Following the third or fifth incorrect attempt to sign a record, that user's signature permissions to that specific data file are permanently deactivated. A warning message appears on the GX/AS station screen. An administrator can reactivate the user for access to subsequent data and GX/AS functions but cannot reactivate the user permissions to that specific batch. This allows the user's signature information to remain secure from tampering in both the GX/AS and SMARTDAC+ standard software environments. Should that individual absolutely need to sign that particular data file, a printed report can be created that can be manually signed by any user.

> Administrative Alert/Procedural Control: At least two administrators should be configured at all times. If an unauthorized attempt to use an administrator's user information is detected, that administrator's access permissions will be deactivated as with a routine user. Unless another administrator has been previously configured, no further administrative access to the unit will be allowed.

A permanent record of all notifications of unauthorized attempts at use and who acknowledged and reset those messages is maintained as part of the GX/AS audit trail records. Thus, if there is ever any question related to user access or signature applications, an administrator can review that data to determine any needed corrective action.

5. Other Procedural Controls

Documentation

Complete system documentation may include standard operating procedures, specifications and validation documents, training records, and any other company policy documents that applies to the processes monitored by the GX/AS. This documentation may be paper-based or electronic. Regardless of the media, appropriate controls over system documentation must be established to assure controlled distribution and revision and change control procedures. Revision and change control procedures must include an audit trail that documents changes chronologically. (21 CFR 11.10(k))

The actual controls implemented will depend on a company's specific documentation systems. Because documents are frequently stored and modified in electronic form but routinely accessed in either electronic or paper form, controls should encompass both types of media. Any associated documentation meeting the definition of an electronic record must also be kept in a manner compliant to Part 11. Access and revisions to paper documents pertaining to electronic records systems must still be controlled in accordance with Part 11.10(k).

Yokogawa SMARTDAC+ Security Functions 21 CFR § 11 Compliance Summary Table

21 CFR § 11 Reference	Meet Requirement?		Comments
	YES	NO	
Controls for Closed Systems			
Persons who use closed systems to create,modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity,and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. 21 CFR § 11.10	YES		The GX/AS employs measures to limit system access to assigned users, and stores data in proprietary binary format, providing a high level of security. There are no available means to change saved data through the GX/AS. The SMARTDAC+ standard software performs a CRC check on each data file to alert the user if the data file has been altered. Electronic signatures applied using the GX/AS or SMARTDAC+ standard software cannot be removed. Controlled user access permissions prevent a user from applying anyone's electronic signature other than their own.
Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. 21 CFR § 11.10 (a)	YES		An optional, Installation/Configuration/Function Verification package is provided that can be used in conjunction with an end user's own operational policies and procedures to meet the requirements for validation of this system.
The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. 21 CFR § 11.10 (b)	YES		GX/AS Display and Event data files are stored in a proprietary Yokogawa binary protocol. These files include audit trail data. Yokogawa Viewer software displays and prints data in human readable form. The files can be easily copied for backups, archiving, inspection, and review.
Protection of records to enable their accurate and ready retrieval throughout the records retention period. 21 CFR § 11.10 (c)	YES		GX/AS storage media can be archived for long-term storage and retrieval, or files can be copied to other long-term archive media such as CDROM. Viewer software can be stored on CDROM with the data files to ensure long-term retention of compatible viewing software. There are no available means to change saved data through the GX/AS or SMARTDAC+ standard software.
Limiting system access to authorized individuals. 21 CFR §11.10 (d)	YES		The GX/AS supports a three-level access authorization feature using User Name, User ID, and Password. Up to 100 users can be registered and divided as needed into system administrators or standard users.
Use of secure, computer-generated, timestamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period for at least as long as that required for the subject electronic records and shall be available for agency review and copying. 21 CFR § 11.10 (e)	YES		The GX/AS maintains records of all alarms, alarm acknowledgements, error messages (including unauthorized attempts at access), changes to configuration and calculation settings, and current user authorization levels in binary files. These files can be viewed through the SMARTDAC+ standard software but cannot be changed by users or administrators. Each log created by the GX/AS is linked to the next data file created after the change. The logs are copied automatically whenever the original data file is copied, and they are transferred to the FTP server for long-term storage along with the associated data file.

Yokogawa SMARTDAC+ Advanced Security Functions 21 CFR § 11 Compliance Summary Table

21 CFR § 11 Reference	Meet Requirement?		Comments
	YES	NO	
Controls for Closed Systems			
Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate. 21 CFR § 11.10 (f)	YES		Data can be reviewed and signed only after the collection has been stopped. If a data set is collected in a batch comprised of more than one data file, that data can not be signed unless all associated files are present.
Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. 21 CFR § 11.10 (g)	YES		The GX/AS supports two or three-level access authorization feature using User Name, User ID (selectable), and Password. The same authority checks are applied at the time of electronic signature affixation.
Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source data input or operational instruction. 21 CFR § 11.10 (h)	YES		The GX/AS functions as a closed system that can be configured at the local user interface. Acquired GX/AS data can be sent to a network directory via a one-way secure interface incorporating available network security features such as user ID and password verification.
Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks. 21 CFR § 11.10 (i)	N/A		Documentation of training and user qualifications is the responsibility of the individual organization. Yokogawa provides operating manuals for each GX/AS and the SMARTDAC+ standard software that can be incorporated into a company's own training procedures.
The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification. 21 CFR § 11.10 (j)	N/A		Written policies holding individuals accountable for actions performed under their electronic signatures are the responsibility of each company. The GX/AS provides a secure electronic signature option the will facilitate compliance in conjunction with a company's internal procedures.
Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and c-hange control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation. 21 CFR § 11.10 (k)	N/A		Procedures for preparation and control of documentation must be established by each individual company.

Yokogawa SMARTDAC+ Advanced Security Functions 21 CFR § 11 Compliance Summary Table

21 CFR § 11 Reference	Meet Requirement?		Comments
	YES	NO	
Controls for Open Systems			
Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in §11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. 21 CFR § 11.30	N/A		The GX/AS is a closed system. Access to records is controlled by the same persons responsible for the content of those records.
Signature Manifestations			
Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: The printed name of the signer; The date and time when the signature was executed; and The meaning (such as review, approval, responsibility, or authorship) associated with the signature. The items identified [above] shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout). 21 CFR § 11.50	YES		The user name, and date and time of signing are automatically linked to the signed record when the signature is affixed. The user must choose either “Pass” or “Fail” and has the additional option of entering a customized text message for each signature. The electronic signature is linked to the record and can not be deleted. All information associated with the electronic signature is available for review both at the GX/AS and through the SMARTDAC+ standard software via electronic display or printout.
Signature/Record Linking			
Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means. 21 CFR § 11.70	YES		Each electronic signature is permanently linked to the associated data set. Up to three (3) electronic signatures can be applied to each file. Because the signature is permanently associated with the data file that is stored in a proprietary binary format, it is not possible to either remove or copy any electronic signatures.
Electronic Signatures			
Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else. 21 CFR § 11.100 (a)	YES		The GX/AS uses the same permission levels used at login to apply electronic signatures. Thus, the electronic signature is always based on a unique user name, ID, and password combination.
Before an organization establishes, assigns, certifies, or otherwise sanctions an individual’s electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual. 21 CFR § 11.100 (b)	N/A		These controls must be implemented by the individual company.

Yokogawa SMARTDAC+ Advanced Security Functions 21 CFR § 11 Compliance Summary Table

21 CFR § 11 Reference	Meet Requirement?		Comments
	YES	NO	
Electronic Signatures			
Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures. 21 CFR § 11.100 (c)	N/A		This certification must be submitted to the FDA by the individual company.
The certification shall be submitted in paper form with a traditional handwritten signature, to the Office of Regional Operations (HFC-100). 21 CFR § 11.100 (c)(1)	N/A		This certification must be submitted to the FDA by the individual company.
Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature. 21 CFR § 11.100 (c)(2)	N/A		This certification must be submitted to the FDA by the individual company.
Electronic Signature Components and Controls			
Employ at least two distinct identification components such as an identification code and password. When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic use components; subsequent signings shall be executed using at least one electronic signature comp onent that is only executable by, and designed to be used only by, the individual. When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. 21 CFR § 11.200	YES		The GX/AS allows for either two or three identification components, either a user ID/password or user name/user ID/password combination. Each combination must be unique. Each signing requires that each component of the electronic signature be entered manually by the user.
Electronic signatures that are not based upon biometrics shall: Be used only with their genuine owners: and Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals. 21 CFR § 11.200	YES		Passwords and user IDs can not be viewed by other users. Passwords are stored in encrypted format and can not be viewed by administrators, only re-set to the original default. The original default is a pre-expired password that must be changed by the user immediately upon initial login before performing any actions on the GX/AS.
Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners. 21 CFR § 11.200	N/A		The GX/AS employs a combination of password and user identification for electronic signatures. It does not use biometric signatures.

Yokogawa SMARTDAC+ Advanced Security Functions 21 CFR § 11 Compliance Summary Table

21 CFR § 11 Reference	Meet Requirement?		Comments
	YES	NO	
Controls for Identification Codes/Passwords			
Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password. Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging). 21 CFR § 11.300	YES		The GX/AS does not allow duplication of User name and Password or User ID and Password combinations. Passwords can be set for automatic expirations of OFF, 1, 3, or 6 months.
Such controls [for identification codes and passwords] shall include: Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls. 21 CFR § 11.300	YES		An Administrator can disable an existing user if an unauthorized attempt at use is detected. Written procedures would need to include the specific controls for maintaining, issuing, testing, and tracking the assigned identification codes and passwords. Tokens and cards are not used.
Such controls [for identification codes and passwords] shall include: Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at the unauthorized use to the system security unit, and, as appropriate, to organizational management. 21 CFR § 11.300	YES		A user's access will be disabled after three (3) or five (5) failed login attempts. This action is logged for audit trail. If, following successful login, the GX/AS detects three (3) or five (5) incorrect attempts to apply an electronic signature to a file, all electronic signature access to that data file will be automatically disabled. The data may still be printed and signed using traditional hand-written signatures. When the GX/AS detects an unauthorized attempt at use, a notification symbol appears on the screen that can only be cleared by an administrator. Authorized data collection sequences will not be interrupted. Additional email notification and/or relay activation for remote notification of user lockout are also available.
Such controls [for identification codes and passwords] shall include: Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner. 21 CFR § 11.300	N/A		Tokens and cards are not used.

Revision Information

Title : SMARTDAC+ Advanced Security Functions White Paper for FDA 21 CFR Part
Manual number : TI 04L51B01-04EN

May 2014/1st Edition
Newly published

Written by Yokogawa Electric Corporation
Published by Yokogawa Electric Corporation
2-9-32 Nakacho, Musashino-shi, Tokyo 180-8750, JAPAN